

# COMPUTING FUNCTIONS ON JACOBIANS AND THEIR QUOTIENTS

JEAN-MARC COUVEIGNES AND TONY EZOME

**ABSTRACT.** We show how to efficiently evaluate functions on Jacobian varieties and their quotients. We deduce an algorithm to compute  $(l, l)$  isogenies between Jacobians of genus two curves in quasi-linear time in the degree  $l^2$ .

## CONTENTS

1. Introduction	1
2. Functions on Jacobians	3
2.1. Notation	3
2.2. An easy special case	5
2.3. Algorithmic considerations	5
2.4. Number of points on Theta divisors	6
2.5. Determinants	7
2.6. Evaluating Eta functions	8
3. Bases of linear spaces	11
4. Canonical Theta functions	12
4.1. Defining canonical Theta functions	12
4.2. Evaluating canonical Theta functions	13
5. Quotients of Jacobians	15
5.1. Explicit descent	15
5.2. Evaluating functions on $J/V$	16
6. Curves of genus two	16
6.1. Algebraic form of the isogeny	17
6.2. Associated differential system	18
6.3. Computing isogenies	19
7. An example	20
References	22

## 1. INTRODUCTION

We consider the problem of computing the quotient of the Jacobian variety  $J$  of a curve  $C$  by a maximal isotropic subgroup  $V$  in its  $l$ -torsion for  $l$  an odd prime integer. The genus one case has been explored a lot since Vélu [33, 34]. A recent bibliography can be found in [4].

---

*Date:* April 7, 2015.

In this work we first study this problem in general, showing how to quickly design and evaluate standard functions (including Theta functions) on the quotient  $J/V$ . We then turn to the specific case when the dimension  $g$  of  $J$  equals two. In that case, the quotient is, at least generically, the Jacobian of another curve  $D$ . The quotient isogeny induces a map from  $C$  into the Jacobian of  $D$  that can then be described in a compact form: a few rational fractions of degree  $O(l)$ . We explain how to compute  $D$  and the map from  $C$  into the Jacobian of  $D$  in quasi-linear time in the degree  $\#V = l^2$ .

**Plan** In Section 2 we bound the complexity of evaluating standard functions on Jacobians, including Weil functions and algebraic Theta functions. We deduce in Section 3 a bound for the complexity of computing a basis of sections for the bundle associated with a multiple of the natural polarization of  $J$ . We recall the algebraic definition of canonical Theta functions in Section 4 and bound the complexity of evaluating such a function at a given point in  $J$ . Section 5 bounds the complexity of evaluating functions on the quotient of  $J$  by a maximal isotropic subgroup  $V$  in  $J[l]$  when  $l$  is an odd prime different from the characteristic of  $\mathbf{K}$ . Specific algorithms for genus two curves are given in Section 6. A complete example is treated in Section 7.

**Context** The algorithmic aspect of isogenies was explored by V  lu [33, 34] in the context of elliptic curves. He exhibits bases of linear spaces made of Weil functions, then finds invariant functions using traces. V  lu considers the problem of computing the quotient variety once given some finite subgroup. The problem of computing (subgroups of) torsion points is independent and was solved in a somewhat optimal way by Elkies [12] in the genus one case, using modular equations. It is unlikely that modular equations will be of any use to accelerate the computation of torsion points for higher genera, since they all are far too big. Torsion points may be computed by brute force (torsion polynomials), using the Zeta function when it is known [8], or because they come naturally as part of the input (modular curves). We shall not consider this problem and will concentrate on the computation of the isogeny, once given its kernel. The genus one case has been surveyed by Schoof [29] and Lercier-Morain [21]. The genus two case was studied by Dolgachev and Lehavi [11], and Smith [31], who provide a very elegant geometric description. However, the complexity of the resulting algorithm is not given (and is not quasi-linear in the degree anyway). Lubicz and Robert [22, 23] provide general methods for quotienting abelian varieties (not necessarily Jacobians) by maximal isotropic subgroups in the  $l$ -torsion. Their method has quasi-linear complexity  $l^{g(1+o(1))}$  when  $l$  is a sum of two squares. Otherwise it has complexity  $l^{g(2+o(1))}$ . The case of dimension two is treated by Cosset and Robert [7]. They reach complexity  $l^{2+o(1)}$  when  $l$  is the sum of two squares and  $l^{4+o(1)}$  otherwise. However, the input and mainly the output of these methods is quite different from ours. In the dimension two case, we can, and must provide a curve  $D$  of which  $J/V$  is the Jacobian, and an explicit map from  $C$  into the symmetric square of  $D$ . We achieve this goal in quasi-linear time  $l^{2+o(1)}$  for every odd prime  $l \neq p$ .

**Acknowledgements** We thank Damien Robert for his comments on an early version of this work and Qing Liu for interesting discussions about holomorphic differentials. Tony Ezome is supported by the Simons Foundation via the PRMAIS project. Jean-Marc Couveignes is supported by the ‘‘Agence Nationale de la Recherche’’ (project PEACE) and by the cluster of excellence CPU (Numerical certification and reliability). Experiments presented in this paper were carried out using PARI/GP [32] and the PLAFRIM experimental testbed, being developed under

the Inria PlaFRIM development action with support from LABRI and IMB and other entities: Conseil Régional d'Aquitaine, Université de Bordeaux and CNRS.

## 2. FUNCTIONS ON JACOBIANS

Constructing functions on abelian varieties using zero-cycles and divisors is classical [35, 36]. In this section, we bound the complexity of evaluating such functions in the special case of Jacobian varieties. Possible references for the theory of Jacobian varieties are [35, 20, 26, 1].

Section 2.1 sets some notation about Jacobian varieties. Section 2.2 is concerned with a special case of Eta functions : those associated to a function on the curve itself. These functions can be easily evaluated. Section 2.3 recalls well known but important algorithmic results about curves and Jacobians. These algorithmic considerations are of particular interest when the base field  $\mathbf{K}$  is finite. Bounds on the number of points on varieties are useful in this context. We recall in Section 2.4 a simple estimate that will suffice for our purpose. We provide in Section 2.5 a formula for the divisor of certain functions on  $J$  defined using determinants. We deduce an expression for Eta functions as combinations of these determinants. The resulting algorithm for evaluating Eta functions is detailed in Section 2.6.

**2.1. Notation.** We let  $\mathbf{K}$  be a field. Let  $\bar{\mathbf{K}}$  be an algebraic closure of  $\mathbf{K}$ . If  $X$  is a  $\mathbf{K}$ -scheme and if  $\mathbf{L}$  is an extension of  $\mathbf{K}$ , we denote by  $X_{\mathbf{L}}$  the base change  $X \otimes_{\mathbf{K}} \mathbf{L}$  and by  $X(\mathbf{L})$  the set of  $\mathbf{L}$ -points on it. Let  $C$  be a projective, smooth, absolutely integral curve over  $\mathbf{K}$ . Let  $g$  be the genus of  $C$ . We assume that  $g \geq 2$  and we denote by  $\text{Pic}(C)$  the Picard scheme of  $C$ . For every integer  $d$  we denote by  $\text{Pic}^d(C)$  the component of  $\text{Pic}(C)$  representing linear classes of divisors of degree  $d$ . In particular,  $J = \text{Pic}^0(C)$  is the Jacobian variety of  $C$ . By definition of the Picard scheme,  $\mathbf{L}$ -points on  $\text{Pic}(C)$  parameterize linear equivalence classes of divisors on  $C_{\mathbf{L}}$ . We shall make no difference between linear classes of divisors and points on the Picard scheme. The *canonical class* on  $C$  is denoted  $\omega$ . It is represented by a  $\mathbf{K}$ -point on  $\text{Pic}^{2g-2}(C)$  which we call  $\omega$  also. If  $D$  is a divisor on  $C_{\mathbf{L}}$  we denote by  $\iota(D)$  its linear equivalence class, and the corresponding  $\mathbf{L}$ -point on  $\text{Pic}(C)$ . Let  $u$  be an  $\mathbf{L}$ -point on  $\text{Pic}(C)$ . We call

$$t_u : \text{Pic}(C)_{\mathbf{L}} \rightarrow \text{Pic}(C)_{\mathbf{L}}$$

the translation by  $u$ . If now  $D$  is a divisor on  $\text{Pic}(C)_{\mathbf{L}}$  we denote by

$$D_u = t_u(D)$$

the translation of  $D$  by  $u$ . We call  $W \subset \text{Pic}^{g-1}(C)$  the algebraic set representing classes of effective divisors of degree  $g-1$ . The pullback  $[-1]^*W \subset \text{Pic}^{1-g}(C)$  is equal to the translate of  $W$  by  $-\omega$ . We write

$$[-1]^*W = W_{-\omega}.$$

If there exists a  $\mathbf{K}$ -rational point  $\theta$  in  $\text{Pic}^{g-1}(C)$  such that

$$2\theta = \omega,$$

then we say that  $\theta$  is a *Theta characteristic*. See [1, Appendix B, §3]. Two such Theta characteristics differ by a 2-torsion point in  $J$ . The translate  $W_{-\theta}$  is a divisor on  $J$ . One has

$$(1) \quad [-1]^*W_{-\theta} = W_{-\theta}.$$

The divisor  $W_{-\theta}$  is said to be *symmetric*. We assume that we are given a  $\mathbf{K}$ -rational point  $O$  on  $C$ , and denote by

$$o = \iota(O)$$

its linear equivalence class. This is a  $\mathbf{K}$ -point on  $\text{Pic}^1(C)$ . The translate  $W_{-(g-1)o}$  is a divisor on  $J$ . We set

$$\kappa = \omega - 2(g-1)o \in J(\mathbf{K}).$$

We have

$$[-1]^* W_{-(g-1)o} = W_{-(g-1)o-\kappa}.$$

We set

$$\vartheta = \theta - (g-1)o \in J(\mathbf{K})$$

and check that

$$2\vartheta = \kappa.$$

Given  $D$  a divisor on  $C$  we write  $L(D)$  for the linear space  $H^0(C, \mathcal{O}_C(D))$  and

$$\ell(D) = \dim(H^0(C, \mathcal{O}_C(D))).$$

Let  $\mathbf{u} = \sum_{1 \leq i \leq I} e_i [u_i]$  be a zero-cycle on  $J_{\bar{\mathbf{K}}}$ . So  $(e_1, e_2, \dots, e_I) \in \mathbf{Z}^I$  and  $(u_1, \dots, u_I) \in J(\bar{\mathbf{K}})^I$ . We set

$$s(\mathbf{u}) = \sum_{1 \leq i \leq I} e_i u_i \in J(\bar{\mathbf{K}}) \text{ and } \deg(\mathbf{u}) = \sum_{1 \leq i \leq I} e_i \in \mathbf{Z}.$$

Let  $D$  be a divisor on  $J_{\bar{\mathbf{K}}}$ . The divisor  $\sum_{1 \leq i \leq I} e_i D_{u_i} - D_{s(\mathbf{u})} - (\deg(\mathbf{u}) - 1)D$  is principal. Let  $y$  be a point in  $J(\bar{\mathbf{K}})$  not in the support of this divisor. Call  $\eta_D[\mathbf{u}, y]$  the unique function on  $J_{\bar{\mathbf{K}}}$  having divisor

$$(\eta_D[\mathbf{u}, y]) = \sum_{1 \leq i \leq I} e_i D_{u_i} - D_{s(\mathbf{u})} - (\deg(\mathbf{u}) - 1)D$$

and such that

$$\eta_D[\mathbf{u}, y](y) = 1.$$

This definition is additive in the sense that

$$(2) \quad \eta_D[\mathbf{u} + \mathbf{v}, y] = \eta_D[\mathbf{u}, y] \cdot \eta_D[\mathbf{v}, y] \cdot \eta_D[[s(\mathbf{u})] + [s(\mathbf{v})], y]$$

whenever it makes sense. If  $D$ ,  $y$ , and  $\mathbf{u}$  are defined over  $\mathbf{K}$  then  $\eta_D \in \mathbf{K}(J)$ . We write

$$\eta_D[\mathbf{u}] \in \mathbf{K}(J)^*/\mathbf{K}^*$$

when we consider an Eta function up to a multiplicative scalar.

Equation (2) allows us to evaluate Eta functions by pieces: we first treat a few special cases and then explain how to combine them to efficiently evaluate any Eta function. We shall see in Sections 4 and 5 that many interesting functions on  $J$  can be expressed as combinations of Eta functions. In this paper we shall be firstly interested in the special case  $D = W_{-(g-1)o}$ . We omit the subscript in that case, and write  $\eta[\mathbf{u}, y]$  rather than  $\eta_{W_{-(g-1)o}}[\mathbf{u}, y]$ .

**2.2. An easy special case.** Let  $f$  be a non-zero function in  $\mathbf{K}(C)$ . Following [9] one can naturally associate to  $f$  a function  $\alpha[f]$  in  $\mathbf{K}(J)$  in the following way. We assume that  $f$  has degree  $d$  and divisor

$$(f) = \sum_{1 \leq i \leq d} Z_i - \sum_{1 \leq i \leq d} P_i.$$

We call  $z_i = \iota(Z_i)$  (resp.  $p_i = \iota(P_i)$ ) the  $\bar{\mathbf{K}}$ -points in  $\text{Pic}^1(C)$  representing the linear equivalence classes of the  $Z_i$  (resp. the  $P_i$ ). Let  $x$  be a point in  $J(\mathbf{K})$  such that  $x \notin W_{p_i - gO}$  for every  $1 \leq i \leq d$ . In particular,  $\ell(x + gO) = 1$ . Indeed every special divisor class of degree  $g$  belongs to  $W_{\iota(P)}$  for every point  $P$  on  $C$  since the corresponding linear series has positive projective dimension and we can find a divisor in it containing any given  $P$ . Let  $D_x$  be the unique effective divisor of degree  $g$  on  $C$  such that  $D_x - gO$  belongs to the class  $x$ . Write  $D_x = D_1 + D_2 + \dots + D_g$  and set

$$(3) \quad \alpha[f](x) = f(D_1) \cdot f(D_2) \cdot \dots \cdot f(D_g).$$

The divisor of  $\alpha[f]$  is

$$(\alpha[f]) = \sum_{1 \leq i \leq d} W_{z_i - gO} - \sum_{1 \leq i \leq d} W_{p_i - gO}.$$

Let  $y$  be a point in  $J(\mathbf{K})$  such that  $y \notin W_{p_i - gO}$  and  $y \notin W_{z_i - gO}$  for every  $1 \leq i \leq d$ . Then

$$\alpha[f](x)/\alpha[f](y) = \eta\left[\sum_{1 \leq i \leq d} [z_i - o] - \sum_{1 \leq i \leq d} [p_i - o], y\right](x).$$

This provides an algorithm to evaluate  $\eta[u, y]$  in the special case when  $u$  is a zero-cycle on  $J$  with support contained in  $t_{-o}(\iota(C)) \subset J$ .

**2.3. Algorithmic considerations.** Having described in Section 2.2 a first method to evaluate Eta functions in some special case, we bound the complexity of this method. We take this opportunity to set some notation and convention.

**2.3.1. Convention.** In this text, the notation  $\mathfrak{D}$  stands for a positive absolute constant. Any statement containing this symbol becomes true if the symbol is replaced in every occurrence by some large enough real number. Similarly, the notation  $\epsilon(x)$  stands for a real function of the real parameter  $x$  alone, belonging to the class  $o(1)$ .

**2.3.2. Operations in  $\mathbf{K}$ .** The time needed for one operation in  $\mathbf{K}$  is a convenient unit of time. Let  $\mathbf{L}$  be a monogene finite  $\mathbf{K}$ -algebra of degree  $d$ . We will assume that  $\mathbf{L}$  is given as a quotient  $\mathbf{K}[x]/f(x)$  where  $f(x)$  is a polynomial in  $\mathbf{K}[x]$ . Every operation in  $\mathbf{L}$  requires  $d^{1+\epsilon(d)}$  operations in  $\mathbf{K}$ . When  $\mathbf{K}$  is a finite field with cardinality  $q$ , every operation in  $\mathbf{K}$  requires  $(\log q)^{1+\epsilon(q)}$  elementary operations.

**2.3.3. Operations in  $J(\mathbf{K})$ .** We assume that  $C$  is given in a reasonable way: for example a plane model with degree polynomial in the genus  $g$ . Elements in  $J(\mathbf{K})$  are classically represented by divisors on  $C$ . We can also use Makdisi's representation [18] which is more efficient. For our purpose it will be enough to know that one operation in  $J(\mathbf{K})$  requires  $g^{\mathfrak{D}}$  operations in  $\mathbf{K}$  that is  $g^{\mathfrak{D}} \cdot (\log q)^{1+\epsilon(q)}$  elementary operations when  $\mathbf{K}$  is a field with  $q$  elements. Given two effective divisors  $D$  and  $E$  with degrees  $d$  and  $e$  respectively, we are able to compute a basis of  $L(D - E)$  at the expense of  $(gde)^{\mathfrak{D}}$  operations in  $\mathbf{K}$ . The Brill-Noether algorithm reduces all theses algorithmic problems to the analysis of the singularities of the given curve. This is classically

achieved by blowing up or using series expansions, but none of these method is fully satisfactory: The complexity of blowing up is not well understood in the worst cases; and computing series expansions is only possible when the characteristic of  $\mathbf{K}$  is zero or large enough. Work by Hess [16], using general normalization algorithms, provides a satisfactory algorithm in general. Possible references for these algorithms are Hess [16], Makdisi [18], Diem [10], or the quick account at the beginning of [8].

**2.3.4. Evaluating  $\alpha[f]$ .** We are given a function  $f$  in  $\mathbf{K}(C)$ . We are given a class  $x$  in  $J(\mathbf{K})$ , represented by  $D_x - gO$  where  $D_x$  is effective with degree  $g$ . We may see  $D_x$  as a zero-dimensional scheme over  $\mathbf{K}$ , and call  $\mathbf{K}[D_x]$  the associated affine  $\mathbf{K}$ -algebra. We assume that  $D_x$  does not meet the poles of  $f$ . Let  $P$  be the generic point on  $D_x$ . Then  $f(P)$  belongs to  $\mathbf{K}[D_x]$  and its norm over  $\mathbf{K}$  is  $\alpha[f](x)$  according to the definition given in Equation (3). Thus we can compute  $\alpha[f](x)$  at the expense of  $(gd)^{\mathfrak{D}}$  operations in  $\mathbf{K}$ , where  $g$  is the genus of  $C$  and  $d$  is the degree of  $f$ .

**2.4. Number of points on Theta divisors.** We recall a rough but very general and convenient upper bound for the number of points in algebraic sets over finite fields. This bound was proved in [15, Proposition 12.1] by Lachaud and Ghorpade. We shall use it to estimate the probability of success of some of the algorithms presented in this paper.

**Lemma 1** (Rough bound for the number of points). *Let  $\mathbf{K}$  be a field with  $q$  elements. Let  $X$  be a projective algebraic set over  $\mathbf{K}$ . Let  $n$  be the maximum of the dimensions of the  $\mathbf{K}$ -irreducible components of  $X$ . Let  $d$  be the sum of the degrees of the  $\mathbf{K}$ -irreducible components of  $X$ . Then*

$$|X(\mathbf{K})| \leq d(q^n + q^{n-1} + \cdots + q + 1).$$

Let  $\mathbf{K}$  be a finite field with cardinality  $q$  and  $C$  a curve over  $\mathbf{K}$  and  $O$  a  $\mathbf{K}$ -rational point on  $C$  and  $J$  the Jacobian of  $C$ . We assume that the genus  $g$  of  $C$  is at least 2. Set  $\iota(O) = o \in \text{Pic}^1(C)$ . Recall that  $W_{-g(o-1)}$  is the algebraic subset of  $J$  consisting of all classes  $\iota(A - (g-1)O)$  where  $A$  is an effective divisor with degree  $g-1$ . Let  $D$  be an algebraic subset of codimension one in  $J$ . We assume that  $D$  is algebraically equivalent to  $kW_{-(g-1)o}$ . Set  $l = \max(3, k)$ . The divisor  $E = D + (l-k)W_{-(g-1)o}$  is algebraically equivalent to  $lW_{-(g-1)o}$ . After base change to  $\bar{\mathbf{K}}$  it becomes linearly equivalent to a translate of  $lW_{-(g-1)o}$ . Since every translate of  $W_{-(g-1)o}$  is ample [28, Chapter II, §6] and  $l \geq 3$  we deduce [28, Chapter III, §17] that  $E$  is very ample. We now apply Lemma 1 to the hyperplane section  $E$ . Its dimension is  $n = g-1$  and its degree  $d$  is

$$E^g = l^g (W_{-(g-1)o})^g = l^g \cdot g!$$

according to Poincaré's formula [1, Chapter I, §5]. So  $|D(\mathbf{K})| \leq |E(\mathbf{K})| \leq l^g \cdot (g!) \cdot (q^{g-1} + q^{g-2} + \cdots + q + 1) \leq g \cdot (g!) \cdot l^g \cdot q^{g-1}$ . On the other hand, according to [19, Théorème 2], the cardinality of  $J(\mathbf{K})$  is at least  $q^{g-1}(q-1)^2(q+1)^{-1}(g+1)^{-1}$ . So the proportion  $D(\mathbf{K})/J(\mathbf{K})$  is  $\leq g^{\mathfrak{D}g} l^g / q$ .

**Lemma 2** (Number of points on divisors). *Let  $\mathbf{K}$  be a finite field with  $q$  elements and  $C$  a curve of genus  $g \geq 2$  over  $\mathbf{K}$ . Let  $J$  be the Jacobian of  $C$ . Let  $O$  be a  $\mathbf{K}$ -point on  $C$  and  $o$  the corresponding class in  $\text{Pic}^1(C)$ . Let  $D \subset J$  be an algebraic subset of codimension one, algebraically equivalent to  $kW_{-(g-1)o}$  for  $k \geq 1$ . Set  $l = \max(3, k)$ . The number of  $\mathbf{K}$ -rational*

points on  $D$  is bounded from above by  $g.(g!).l^g.q^{g-1}$ . The ratio  $|D(\mathbf{K})|/|J(\mathbf{K})|$  is bounded from above by  $g^{\mathfrak{D}g}l^g/q$ .

**2.5. Determinants.** The evaluation method presented in Section 2.3 only applies to Alpha functions introduced in Section 2.2. These Alpha functions form a subfamily of Eta functions. Mascot introduced in [24] an efficient evaluation method that applies to another interesting subfamily.

One can also define and evaluate functions on  $J$  using determinants. See [2, 13, 30]. We shall see that every Eta function can be expressed as a combination of Alpha functions, as in Section 2.2, and determinants. Let  $D$  be a divisor on  $C$  with degree  $d \geq 2g - 1$ . Set

$$n = \ell(D) = d - g + 1.$$

Let  $f = (f_k)_{1 \leq k \leq n}$  be a basis of  $L(D)$ . For  $P = (P_l)_{1 \leq l \leq n}$  in  $C^n$  disjoint from the positive part of  $D$  we set

$$\beta[f](P) = \det(f_k(P_l))_{k,l}$$

and thus define a function  $\beta[f]$  on  $C^n$ . Call

$$j : C^n \rightarrow \text{Pic}^n(C)$$

the Jacobi integration map. It maps  $(P_1, \dots, P_n)$  onto the class of  $P_1 + \dots + P_n$ . We call

$$\pi_l : C^n \rightarrow C$$

the projection onto the  $l$ -th factor. For  $1 \leq i < j \leq n$  we set

$$\Delta_{i,j} = \{(P_1, \dots, P_n) | P_i = P_j\} \subset C^n.$$

Let

$$\Delta = \cup_{1 \leq i < j \leq n} \Delta_{i,j} \subset C^n$$

be the full diagonal. The divisor of  $\beta[f]$  is

$$(4) \quad (\beta[f]) = \Delta + j^*(t_{\iota(D)}([-1]^*W)) + \sum_{1 \leq l \leq n} \pi_l^*(-D)$$

where  $t_{\iota(D)}([-1]^*W) = W_{\iota(D)-\omega} \subset \text{Pic}^n(C)$  is the translate of  $[-1]^*W$  by the class of  $D$ . When  $\mathbf{K}$  has characteristic zero Equation 4 results from [13, Proposition 2.16]. For general  $\mathbf{K}$ , a Galois theoretic proof is given by Shepherd-Barron in [30, Corollary 4.2]. Roughly speaking the term  $\Delta$  in Equation (4) means that the determinant vanishes when  $P_i = P_j$  because there are two equal columns in that case. The  $\sum_{1 \leq l \leq n} \pi_l^*(-D)$  says that poles of the determinant come from poles of the coefficients in it. The term  $j^*(t_{\iota(D)}([-1]^*W))$  says that if the  $n$  points  $P_1, \dots, P_n$ , are distinct, the determinant vanishes if and only if there exists a non-zero function in  $L(D)$  vanishing at  $P_1, \dots, P_n$ . And this means that  $D$  is linearly equivalent to  $P_1 + \dots + P_n$  plus some effective divisor of degree  $g - 1$ .

We now assume that we have a collection of divisors  $D = (D^{(i)})_{1 \leq i \leq I}$ . We assume that all  $D^{(i)}$  have degree  $d = 2g - 1$ . So  $n = \ell(D^{(i)}) = g$ . We are given a vector of integers  $e = (e_i)_{1 \leq i \leq I}$  such that  $\sum_{1 \leq i \leq I} e_i = 0$ . For every  $i$  we choose a basis  $f^{(i)} = (f_k^{(i)})_{1 \leq k \leq g}$  of  $L(D^{(i)})$ . We assume that

$\sum_{1 \leq i \leq I} e_i D^{(i)}$  is the (principal) divisor of some function  $h$  on  $C$ . We call  $\alpha[h]$  the function on  $J$  associated with  $h$ , as constructed in Section 2.2. We set  $f = (f^{(i)})_{1 \leq i \leq I}$ . Define the function

$$\beta[D, e, f] = \prod_{1 \leq i \leq I} \beta[f^{(i)}]^{e_i}$$

on  $C^g$ . It has divisor

$$(\beta[D, e, f]) = \sum_i e_i \cdot J^*(W_{\iota(D^{(i)}) - \omega}) - \sum_{\substack{1 \leq i \leq I \\ 1 \leq l \leq g}} e_i \cdot \pi_l^*(D^{(i)}).$$

There exists a function  $\beta'[D, e, f]$  on  $\text{Pic}^g(C)$  such that  $\beta[D, e, f] = \beta'[D, e, f] \circ j$ . Indeed, permuting the  $g$  points  $(P_i)_{1 \leq i \leq g}$  multiplies each factor  $\beta[f^{(i)}]$  by the same sign. We call  $\gamma[D, e, f]$  the function on  $J = \text{Pic}^0(C)$  obtained by composing  $\beta'[D, e, f]$  with the translation by  $go$ . The product  $\gamma[D, e, f] \cdot \alpha[h]$  has divisor

$$(\gamma[D, e, f]) + (\alpha[h]) = \sum_i e_i W_{-(g-1)o + u_i},$$

where

$$u_i = \iota(D^{(i)}) - \omega - o \in J(\mathbf{K}).$$

We deduce that

$$(5) \quad \gamma[D, e, f] \cdot \alpha[h] = \eta[\mathbf{u}] \in \mathbf{K}(J)^* / \mathbf{K}^*$$

where  $\mathbf{u} = \sum_i e_i [u_i]$ . This is exactly what we need. Every Eta function decomposes (up to a multiplicative scalar) as the product of a certain number of determinants times some Alpha function, which we know how to compute. In the next Section 2.6 we deduce an algorithm for evaluating Eta functions.

**2.6. Evaluating Eta functions.** We explain how to evaluate Eta functions, using the product decomposition given in Equation (5). We are given  $\mathbf{u} = \sum_{1 \leq i \leq I} e_i [u_i]$  a zero-cycle on  $J$ . We assume that  $u_i \in J(\mathbf{K})$  for  $1 \leq i \leq I$ . We can and will assume without loss of generality that  $\deg(\mathbf{u}) = \sum_i e_i = 0$  and  $s(\mathbf{u}) = \sum_i e_i u_i = 0$ . We are given two classes  $x$  and  $y$  in  $J(\mathbf{K})$ . The class  $x$  is represented by a divisor  $D_x - gO$  where  $D_x$  is effective with degree  $g$ . The class  $y$  is represented similarly by a divisor  $D_y - gO$ . We assume that neither of  $x$  and  $y$  belong to the support of the divisor  $\sum_{1 \leq i \leq I} e_i W_{-(g-1)o + u_i}$ . We want to evaluate  $\eta[\mathbf{u}, y](x)$ .

The algorithm goes as follows.

- (1) For every  $1 \leq i \leq I$ , find an effective divisor  $D^{(i)}$  of degree  $2g - 1$  such that  $D^{(i)}$  does neither meet  $D_x$  nor  $D_y$ , and  $\iota(D^{(i)}) - \omega - o$  is the class  $u_i$ .
- (2) Find a non-zero function  $h$  in  $\mathbf{K}(C)$  with divisor  $\sum_{1 \leq i \leq I} e_i D^{(i)}$ .
- (3) For every  $1 \leq i \leq I$ , compute a basis  $f^{(i)} = (f_k^{(i)})_{1 \leq k \leq g}$  of  $L(D^{(i)})$ .
- (4) Write  $D_x = X_1 + X_2 + \dots + X_g$  and  $D_y = Y_1 + Y_2 + \dots + Y_g$  where  $X_k$  and  $Y_k$  are points in  $C(\bar{\mathbf{K}})$  for  $1 \leq k \leq g$ . For every  $1 \leq i \leq I$ , compute

$$\delta_x^{(i)} = \det(f_k^{(i)}(X_l))_{1 \leq k, l \leq g} \text{ and } \delta_y^{(i)} = \det(f_k^{(i)}(Y_l))_{1 \leq k, l \leq g}.$$

- (5) Compute  $\alpha[h](x)$  and  $\alpha[h](y)$ .



(6) Return

$$\frac{\alpha[h](x)}{\alpha[h](y)} \cdot \prod_{1 \leq i \leq I} (\delta_x^{(i)} / \delta_y^{(i)})^{e_i}.$$

Note that the product above reflects the product in Equation (5). The only difference is that we evaluate at two points  $x$  and  $y$  to fix the multiplicative constant in  $\mathbf{K}^*$ . We now precise every step. In step (1) we assume that the class  $u_i$  is given by a divisor  $U_i - gO$  where  $U_i$  is effective with degree  $g$ . We proceed as in [8, Lemmata 13.1.7-8-9]. We choose a canonical divisor  $K$  on  $C$  and compute  $L(U_i - (g-1)O + K)$ . With every non-zero function  $f$  in this linear space is associated a candidate divisor

$$(f) + U_i - (g-1)O + K$$

for  $D^{(i)}$ . We eliminate the candidates that meet either  $D_x$  or  $D_y$ . The corresponding functions  $f$  belong to a union of at most  $2g$  strict subspaces of  $L(U_i - (g-1)O + K)$ . If the cardinality of  $\mathbf{K}$  is bigger than  $2g$  we find a decent divisor  $D^{(i)}$  by solving inequalities. If  $\mathbf{K}$  is too small, we can replace  $\mathbf{K}$  by a small extension of it. In any case, we find some  $D^{(i)}$  at the expense of  $g^{\mathfrak{D}}$  operations in  $\mathbf{K}$ .

Step (2) is effective Riemann-Roch. It requires  $(g \cdot |e|)^{\mathfrak{D}}$  operations in the base field, where

$$|e| = \sum_{1 \leq i \leq I} |e_i|$$

is the  $\ell^1$ -norm. Step (3) is similar to step (2) and requires  $I \cdot g^{\mathfrak{D}}$  operations in  $\mathbf{K}$ . Step (4) requires some care. Brute force calculation with the  $X_k$  and  $Y_k$  may not be polynomial time in the genus because the degree over  $\mathbf{K}$  of the decomposition field of  $D_x$  and  $D_y$  may be very large. However, if  $\mathbf{K}$  is finite and if  $D_x$  is irreducible over  $\mathbf{K}$ , then this decomposition field has degree  $g$ , which is fine with us. In general, we write  $D_x = \sum_{1 \leq l \leq L} a_l R_l$  where the  $R_l$  are pairwise distinct irreducible divisors and the  $a_l$  are positive integers. We compute a new basis  $(\phi_k)_{1 \leq k \leq g}$  for  $L(D^{(i)})$  which is adapted to the decomposition of  $D_x$  in the following sense: we start with a basis of  $L(D^{(i)} - \sum_{l \geq 2} a_l R_l)$ , we continue with a basis of  $L(D^{(i)} - \sum_{l \geq 3} a_l R_l) / L(D^{(i)} - \sum_{l \geq 2} a_l R_l)$ , we continue with a basis of  $L(D^{(i)} - \sum_{l \geq 4} a_l R_l) / L(D^{(i)} - \sum_{l \geq 3} a_l R_l)$ , and so on. The matrix  $(\phi_k^{(i)}(X_l))_{1 \leq k, l \leq g}$  is block-triangular, so its determinant is a product of  $L$  determinants (one for each  $R_l$ ). We compute each of these  $L$  determinants by brute force and multiply them together. We multiply the resulting product by the determinant of the transition matrix between the two bases.

For step (5) we use the method described in Section 2.3.4. Step (6) seems trivial, but it hides an ultimate difficulty. If  $D_x$  is not simple, then all  $\delta_x^{(i)}$  are zero and there appear artificial indeterminacies in the product  $\prod_i (\delta_x^{(i)})^{e_i}$ . We use a deformation to circumvent this difficulty. We introduce a formal parameter  $t$  and consider the field  $\mathbf{L} = \mathbf{K}((t))$  of formal series in  $t$  with coefficients in  $\mathbf{K}$ . Consider for example the worst case in which  $D_x$  is  $g$  times a point  $A$ . We fix a local parameter  $z_A \in \mathbf{K}(C)$  at  $A$ . We fix  $g$  pairwise distinct scalars  $(a_m)_{1 \leq m \leq g}$  in  $\mathbf{K}$ . In case the cardinality of  $\mathbf{K}$  is  $< g$ , we replace  $\mathbf{K}$  by a small degree extension of it. We denote  $X_1(t), X_2(t), \dots, X_g(t)$ , the  $g$  points in  $C(\mathbf{L})$  associated with the values  $a_1 t, \dots, a_g t$ , of the local parameter  $z_A$ . We perform the calculations described above with  $D_x$  replaced by  $D_x(t) = X_1(t) + \dots + X_g(t)$ ,

and set  $t = 0$  in the result. Since we use a field of series, we care about the necessary  $t$ -adic accuracy. This is the maximum  $t$ -adic valuation of the  $\beta[f^{(i)}](D_x(t))$ . Assuming that  $x$  does not belong to the support of the divisor  $(\eta[u]) = \sum_{1 \leq i \leq I} e_i W_{-(g-1)o+u_i}$ , these valuations all are equal to  $g(g-1)/2$ . So the complexity remains polynomial in the genus  $g$ . In case  $\mathbf{K}$  is a finite field we obtain the theorem below.

**Theorem 1** (Evaluating Eta functions on the Jacobian). *There exists a deterministic algorithm that takes as input*

- a finite field  $\mathbf{K}$  with cardinality  $q$ ,
- a curve  $C$  of genus  $g \geq 2$  over  $\mathbf{K}$ ,
- a collection of  $\mathbf{K}$ -points  $(u_i)_{1 \leq i \leq I}$  on the Jacobian  $J$  of  $C$ ,
- a zero-cycle  $\mathbf{u} = \sum_{1 \leq i \leq I} e_i [u_i]$  on  $J$ , such that  $\deg(\mathbf{u}) = 0$  and  $s(\mathbf{u}) = 0$ ,
- a point  $O$  in  $C(\mathbf{K})$ ,
- and two points  $x, y \in J(\mathbf{K})$ , not in  $\cup_{1 \leq i \leq I} W_{-(g-1)o+u_i}$ .

The algorithm computes  $\eta[\mathbf{u}, y](x)$  in time  $(g \cdot |e|)^{\mathfrak{D}} \cdot (\log q)^{1+\epsilon(q)}$ , where  $|e| = \sum_{1 \leq i \leq I} |e_i|$  is the  $\ell^1$ -norm of  $e$ .

Using fast exponentiation and Equation (2) in the algorithm above, we can evaluate Eta functions in time  $g^{\mathfrak{D}} \cdot I \cdot (\log |e|) \cdot (\log q)^{1+\epsilon(q)}$ . However, this method may fail when one of the arguments  $x$  or  $y$  belongs to the support of the divisor of some intermediate factor. According to Lemma 2 the proportion of such  $x$  in  $J(\mathbf{K})$  is  $\leq g^{\mathfrak{D}g} \cdot I \cdot (\log |e|) / q$ . A fast method that works for a large proportion of the inputs will be enough to us in the sequel.

**Proposition 1** (Fast evaluation of Eta functions on the Jacobian). *There exists a deterministic algorithm that takes as input*

- a finite field  $\mathbf{K}$  with cardinality  $q$ ,
- a curve  $C$  of genus  $g \geq 2$  over  $\mathbf{K}$ ,
- a point  $O$  in  $C(\mathbf{K})$ ,
- a collection of  $\mathbf{K}$ -points  $(u_i)_{1 \leq i \leq I}$  on the Jacobian  $J$  of  $C$ ,
- a zero-cycle  $\mathbf{u} = \sum_{1 \leq i \leq I} e_i [u_i]$  on  $J$ , such that  $\deg(\mathbf{u}) = 0$  and  $s(\mathbf{u}) = 0$ ,
- and two points  $x, y \in J(\mathbf{K})$ , not in  $\cup_{1 \leq i \leq I} W_{-(g-1)o+u_i}$ .

The algorithm returns either FAIL or  $\eta[\mathbf{u}, y](x)$  in time

$$g^{\mathfrak{D}} \cdot I \cdot (\log |e|) \cdot (\log q)^{1+\epsilon(q)},$$

where  $|e| = \sum_{1 \leq i \leq I} |e_i|$  is the  $\ell^1$ -norm of  $e$ .

For given  $\mathbf{K}$ ,  $C$ ,  $\mathbf{u}$ ,  $O$ , there exists a subset  $\mathbf{FAIL}(\mathbf{K}, C, \mathbf{u}, O)$  of  $J(\mathbf{K})$  with density

$$\leq g^{\mathfrak{D}g} \cdot I \cdot \log(|e|) / q$$

and such that the algorithm succeeds whenever neither  $x$  nor  $y$  belongs to  $\mathbf{FAIL}(\mathbf{K}, C, \mathbf{u}, O)$ .

Fast exponentiation for evaluating Weil functions on abelian varieties first appears in work by Miller [25] in the context of pairing computation on elliptic curves.

## 3. BASES OF LINEAR SPACES

Being able to evaluate Eta functions  $\eta[u, y]$  we now consider an integer  $l \geq 2$  and look for a basis of  $H^0(J, \mathcal{O}_J(lW_{-(g-1)o}))$ . A related problem is to pick random functions in this linear space with close enough to uniform probability. We assume that the base field is finite, and use the rough consequences of Weil bounds stated in Section 2.4. Fix two positive coprime integers  $a$  and  $b$  such that  $a + b = l$ . For every  $u$  and  $y$  in  $J(\mathbf{K})$  such that  $y \notin W_{-(g-1)o} \cup W_{-(g-1)o+au} \cup W_{-(g-1)o-bu}$  call  $\tau[u, y]$  the unique function with divisor

$$(\tau[u, y]) = bW_{-(g-1)o+au} + aW_{-(g-1)o-bu} - lW_{-(g-1)o}$$

such that  $\tau[u, y](y) = 1$ . So

$$\tau[u, y] = \eta[b[au] + a[-bu], y].$$

Let  $\tau[u]$  be the class of  $\tau[u, y]$  in  $\mathbf{K}(J)^*/\mathbf{K}^*$ . When  $u$  is an  $l$ -torsion point  $\tau[u] = \eta[l[au]]$  is a level  $l$  Theta function. It is a classical result of the theory of Theta functions that the collection of all  $\eta[l[u]]$  when  $u$  runs over  $J[l](\bar{\mathbf{K}})$  generate  $H^0(J_{\bar{\mathbf{K}}}, \mathcal{O}_{J_{\bar{\mathbf{K}}}}(lW_{-(g-1)o}))$ . See [3, Theorem 3.2.7] in case  $\mathbf{K}$  has characteristic zero and [27, §10] in general, or Section 4 below. So the collection of all  $\tau[u]$  when  $u$  runs over the set  $J[l](\bar{\mathbf{K}})$  is a generating set for  $\mathbf{P}(H^0(J_{\bar{\mathbf{K}}}, \mathcal{O}_{J_{\bar{\mathbf{K}}}}(lW_{-(g-1)o})))$ . So the map  $u \mapsto \tau[u]$  from  $J$  to  $\mathbf{P}(H^0(J, \mathcal{O}_J(lW_{-(g-1)o})))$  is non-degenerate. Hyperplane sections for this map are algebraically equivalent to  $ablW_{-(g-1)o}$ .

We pick a random element  $u$  in  $J(\mathbf{K})$ , using the Monte Carlo probabilistic algorithm given in [8, Lemma 13.2.4]. This algorithm returns a random element  $u$  with uniform probability inside a subgroup of  $J(\mathbf{K})$  with index  $\xi \leq \mathfrak{D}g^{\mathfrak{D}}$ . We then consider the function  $\tau[u, y]$  where  $y$  is any point in  $J(\mathbf{K})$  not in  $W_{-(g-1)o} \cup W_{-(g-1)o+au} \cup W_{-(g-1)o-bu}$ . According to Lemma 2, for every hyperplane  $H$  in  $\mathbf{P}(H^0(J, \mathcal{O}_J(lW_{-(g-1)o})))$ , the proportion of  $u \in J(\mathbf{K})$  such that  $\tau[u]$  belongs to  $H$  is  $\leq (lg)^{\mathfrak{D}g}/q$ . We assume that  $q$  is large enough to make this proportion smaller than  $\leq 1/(2\xi)$ . The probability that  $\tau[u]$  belongs to  $H$  is then  $\leq 1/2$ .

**Proposition 2** (Random functions). *There exists a constant  $\mathfrak{D}$  such that the following is true. There exists a probabilistic Las Vegas algorithm that takes as input*

- three integers  $l \geq 2$ ,  $a \geq 1$ , and  $b \geq 1$ , such that  $a$  and  $b$  are coprime and  $a + b = l$ ,
- a curve  $C$  of genus  $g \geq 2$  over a field  $\mathbf{K}$  with  $q$  elements, such that  $q \geq (lg)^{\mathfrak{D}g}$ ,
- a point  $O$  in  $C(\mathbf{K})$ .

*The algorithm returns a pair  $(u, y)$  in  $J(\mathbf{K})^2$  such that  $\eta[u, y] \in H^0(J, \mathcal{O}_J(lW_{-(g-1)o}))$  is a random function with probability measure  $\mu$  such that  $\mu(H) \leq 1/2$  for every hyperplane  $H$  in  $H^0(J, \mathcal{O}_J(lW_{-(g-1)o}))$ . The algorithm runs in time  $g^{\mathfrak{D}} \cdot (\log l) \cdot (\log q)^{1+\epsilon(q)}$ .*

In order to find a basis of  $H^0(J, \mathcal{O}_J(lW_{-(g-1)o}))$  we take  $I \geq \mathfrak{D} \cdot lg \cdot \log(lg)$  and pick  $I$  random elements  $(u_i)_{1 \leq i \leq I}$  in  $J(\mathbf{K})$  as explained above. For every  $i$  we find a  $y_i$  in  $J(\mathbf{K})$  such that  $y_i \notin W_{-(g-1)o} \cup W_{-(g-1)o+au_i} \cup W_{-(g-1)o-bu_i}$ . We pick another  $I$  elements  $(w_j)_{1 \leq j \leq I}$  such that  $w_j \notin W_{-(g-1)o}$ . We compute  $\tau[u_i, y_i](w_j)$  for every pair  $(i, j)$ . We put the corresponding  $I \times I$  matrix in echelon form. If the rank is  $lg$  we deduce a basis for both  $H^0(J, \mathcal{O}_J(lW_{-(g-1)o}))$  and its dual all at a time.

**Proposition 3** (Basis of  $H^0(J, \mathcal{O}_J(lW_{-(g-1)o}))$ ). *There exists a constant  $\mathfrak{D}$  such that the following is true. There exists a probabilistic Las Vegas algorithm that takes as input*

- *three integers  $l \geq 2$ ,  $a \geq 1$ , and  $b \geq 1$ , such that  $a$  and  $b$  are coprime and  $a + b = l$ ,*
- *a curve  $C$  of genus  $g \geq 2$  over a field  $\mathbf{K}$  with  $q$  elements, such that  $q \geq (lg)^{\mathfrak{D}g}$ ,*
- *a point  $O$  in  $C(\mathbf{K})$ .*

*The algorithm returns  $l^g$  triples  $(u_i, y_i, w_i) \in J(\mathbf{K})^3$  such that  $(\tau[u_i, y_i])_{1 \leq i \leq l^g}$  is a basis of  $H^0(J, \mathcal{O}_J(lW_{-(g-1)o}))$  and  $(w_i)_{1 \leq i \leq l^g}$  is a basis of its dual. The algorithm runs in time*

$$g^{\mathfrak{D}} \cdot (l^g)^{\omega(1+\epsilon(l^g))} \cdot (\log q)^{1+\epsilon(q)}$$

*where  $\omega$  is the exponent in matrix multiplication.*

One finds in [6, Chapter 15] an elegant presentation of the complexity of matrix multiplication, a definition of the exponent  $\omega$ , and a reasonably simple proof of Coppersmith and Winograd's inequality  $\omega < 2.41$ . It is an open question whether  $\omega = 2$ . The current best result in this direction is the proof by Le Gall in [14] that  $\omega < 2.3728639$ .

If the condition  $q \geq (lg)^{\mathfrak{D}g}$  in the Proposition above is not met, we work with a small extension  $\mathbf{L}$  of  $\mathbf{K}$ , then make a descent from  $\mathbf{L}$  to  $\mathbf{K}$  on the result. The resulting basis will consist of traces of Tau functions.

#### 4. CANONICAL THETA FUNCTIONS

Let  $l \geq 3$  be an odd prime. We assume that  $l$  is different from the characteristic  $p$  of  $\mathbf{K}$ . According to Equation (1) the divisor  $W_{-\theta} \subset J$  is symmetric. Let  $\mathcal{L} = \mathcal{O}_J(lW_{-\theta})$  be the sheaf associated to the divisor  $lW_{-\theta}$ . The Theta group  $\mathcal{G}(\mathcal{L})$  fits in the exact sequence

$$1 \rightarrow \mathbf{G}_m \rightarrow \mathcal{G}(\mathcal{L}) \rightarrow J[l] \rightarrow 0.$$

In this section we recall the definition of algebraic Theta functions. Level  $l$  Theta functions belong to  $H^0(J_{\bar{\mathbf{K}}}, \mathcal{O}_{J_{\bar{\mathbf{K}}}}(lW_{-\theta}))$  and they generate it. They are useful to define descent data. We shall need them in Section 5. In this section we bound the complexity of evaluating Theta functions.

**4.1. Defining canonical Theta functions.** We recall the properties of canonical Theta functions as defined e.g. in [3, 3.2] or [27, §3]. We shall see that canonical Theta functions can be characterized more easily when the level  $l$  is odd. For  $u$  in  $J[l](\bar{\mathbf{K}})$  we let  $\theta_u$  be a function on  $J_{\bar{\mathbf{K}}}$  with divisor  $l(W_{-\theta+u} - W_{-\theta})$ . We call

$$\mathbf{a}_u : H^0(J_{\bar{\mathbf{K}}}, \mathcal{O}_{J_{\bar{\mathbf{K}}}}(lW_{-\theta})) \rightarrow H^0(J_{\bar{\mathbf{K}}}, \mathcal{O}_{J_{\bar{\mathbf{K}}}}(lW_{-\theta}))$$

the endomorphism that maps every function  $f$  onto the product of  $\theta_u$  by  $f \circ t_{-u}$ . For the moment  $\theta_u$  and  $\mathbf{a}_u$  are only defined up to a multiplicative scalar. We now normalize both of them. We want the  $l$ -th iterate of  $\mathbf{a}_u$  to be the identity. So  $\theta_u \cdot (\theta_u \circ t_u) \cdot \dots \cdot (\theta_u \circ t_{(l-1)u})$  should be one. We therefore divide  $\theta_u$  by one of the  $l$ -th roots of the above product to ensure that  $\mathbf{a}_u$  has order dividing  $l$ . Now  $\theta_u$  and  $\mathbf{a}_u$  are defined up to an  $l$ -th root of unity. We compare  $[-1] \circ \mathbf{a}_u \circ [-1]$  and  $\mathbf{a}_u^{-1}$ . They differ by an  $l$ -th root of unity  $\zeta$ . Since  $l$  is odd,  $\zeta$  has square root  $\zeta^{(l+1)/2}$ . Dividing  $\mathbf{a}_u$  and  $\theta_u$  by this square root we complete their definition.

**Proposition 4** (Canonical Theta functions). *For every  $u$  in  $J[l](\bar{\mathbf{K}})$  there is a unique function  $\theta_u$  with divisor  $l(W_{-\theta+u} - W_{-\theta})$  such that*

$$(6) \quad \theta_u \cdot (\theta_u \circ t_u) \cdot (\theta_u \circ t_{2u}) \cdots (\theta_u \circ t_{(l-1)u}) = 1$$

and

$$(7) \quad \theta_u \circ [-1] = (\theta_u \circ t_u)^{-1}.$$

Further  $\theta_{-u} = \theta_u \circ [-1]$ . The map  $u \mapsto \theta_u$  is Galois equivariant: for every  $\sigma$  in the absolute Galois group of  $\mathbf{K}$  we have

$$\sigma\theta_u = \theta_{\sigma(u)}.$$

Let  $\mathbf{a}_u$  be the endomorphism

$$\mathbf{a}_u : H^0(J_{\bar{\mathbf{K}}}, \mathcal{O}_{J_{\bar{\mathbf{K}}}}(lW_{-\theta})) \longrightarrow H^0(J_{\bar{\mathbf{K}}}, \mathcal{O}_{J_{\bar{\mathbf{K}}}}(lW_{-\theta}))$$

$$f \longmapsto \theta_u \cdot (f \circ t_{-u}).$$

we have  $\mathbf{a}_u^l = 1$  and  $[-1] \circ \mathbf{a}_u \circ [-1] = \mathbf{a}_{-u} = \mathbf{a}_u^{-1}$ . The map  $u \mapsto \mathbf{a}_u$  is Galois equivariant.

*Proof.* There only remains to prove the equivariance property. It follows from the equivariance of conditions (6) and (7).  $\square$

For  $u$  and  $v$  in  $J[l](\bar{\mathbf{K}})$  we write

$$e_l(u, v) = \mathbf{a}_u \mathbf{a}_v \mathbf{a}_u^{-1} \mathbf{a}_v^{-1} \in \mu_l$$

for the commutator pairing and

$$f_l(u, v) = \sqrt{e_l(u, v)} = (e_l(u, v))^{\frac{l+1}{2}}$$

for the half pairing. We check that

$$(8) \quad \theta_{u+v} = f_l(u, v) \cdot \theta_v \cdot (\theta_u \circ t_{-v}) = f_l(v, u) \cdot \theta_u \cdot (\theta_v \circ t_{-u}),$$

and

$$\mathbf{a}_{u+v} = f_l(u, v) \cdot \mathbf{a}_v \mathbf{a}_u = f_l(v, u) \cdot \mathbf{a}_u \mathbf{a}_v,$$

and

$$\mathbf{a}_u(\theta_v) = f_l(u, v) \cdot \theta_{u+v}.$$

**4.2. Evaluating canonical Theta functions.** We relate the canonical Theta functions to the Eta functions introduced in Section 2 and show how to evaluate them. We assume that we are given  $u$  and  $x$  in  $J(\mathbf{K})$  with  $lu = 0$ , and we want to evaluate  $\theta_u(x)$ . We assume that  $x \notin W_{-\theta}$ . Since  $l$  is odd we set

$$v = \frac{l+1}{2} \cdot u \in J(\mathbf{K}).$$

We deduce from Equation (8) that

$$\theta_u(x) = \theta_v(x) \cdot \theta_v(x - v)$$

provided that  $x \notin W_{-\theta+v}$ . On the other hand, we deduce from Equation (7) that

$$\theta_v(x) \cdot \theta_v(v-x) = 1$$

provided that  $x \notin W_{-\theta} \cup W_{-\theta+v}$ . So

$$\theta_u(x) = \theta_v(x-v)/\theta_v(v-x)$$

provided that  $x \notin W_{-\theta} \cup W_{-\theta+v}$ . Since  $\theta_v$  and  $\eta[l[v]] \circ t_\vartheta$  have the same divisor we deduce that

$$(9) \quad \theta_u(x) = \eta[l[v], v-x+\vartheta](x-v+\vartheta)$$

provided that  $x \notin W_{-\theta} \cup W_{-\theta+v}$ .

Thanks to Equation (9), evaluating a canonical Theta function  $\theta_u(x)$  reduces to the evaluation of one Eta function. This can be done as explained in Section 2.6. Applying Theorem 1 we find that the computational cost is bounded from above by  $(gl)^\mathfrak{D} \cdot (\log q)^{1+\epsilon(q)}$ .

**Proposition 5** (Evaluating canonical Theta functions). *There exists a deterministic algorithm that takes as input*

- a finite field  $\mathbf{K}$  with characteristic  $p$  and cardinality  $q$ ,
- a curve  $C$  of genus  $g \geq 2$  over  $\mathbf{K}$ ,
- a Theta characteristic  $\theta$  defined over  $\mathbf{K}$ ,
- an odd prime integer  $l \neq p$ ,
- and two points  $u$  and  $x$  in  $J(\mathbf{K})$  such that  $lu = 0$ , and

$$x \notin W_{-\theta} \cup W_{-\theta+v},$$

where

$$v = \frac{l+1}{2} \cdot u \in J(\mathbf{K}).$$

The algorithm computes  $\theta_u(x)$  in time  $(gl)^\mathfrak{D} \cdot (\log q)^{1+\epsilon(q)}$ .

According to Proposition 1 we can accelerate the computation using fast exponentiation. The resulting algorithm will fail when the argument  $x$  belongs to the support of the divisor of some intermediate factor.

**Proposition 6** (Fast evaluation of canonical Theta functions). *There exists a deterministic algorithm that takes as input*

- a finite field  $\mathbf{K}$  with cardinality  $q$  and characteristic  $p$ ,
- a curve  $C$  of genus  $g \geq 2$  over  $\mathbf{K}$ ,
- a Theta characteristic  $\theta$  defined over  $\mathbf{K}$ ,
- an odd prime integer  $l \neq p$ ,
- and two points  $u$  and  $x$  in  $J(\mathbf{K})$  such that  $lu = 0$ .

The algorithm returns either FAIL or  $\theta_u(x)$  in time  $g^\mathfrak{D} \cdot (\log q)^{1+\epsilon(q)} \cdot \log l$ . For given  $\mathbf{K}$ ,  $C$ ,  $\theta$ ,  $u$ , there exists a subset  $\mathbf{FAIL}(\mathbf{K}, C, \theta, u)$  of  $J(\mathbf{K})$  with density  $\leq g^{\mathfrak{D}g} \cdot (\log l)/q$  and such that the algorithm succeeds whenever  $x$  does not belong to  $\mathbf{FAIL}(\mathbf{K}, C, \theta, u)$ .

## 5. QUOTIENTS OF JACOBIANS

Let  $V \subset J[l]$  be a maximal isotropic subgroup for the commutator pairing, let  $f : J \rightarrow J/V$  be the quotient map. Let  $\mathcal{L} = \mathcal{O}_J(lW_{-\theta})$ . The map  $v \mapsto \mathbf{a}_v$  is a homomorphism  $V \rightarrow \mathcal{G}(\mathcal{L})$  lifting the inclusion  $V \subset J[l]$ . This canonical lift provides a descent datum for  $\mathcal{L}$  onto  $J/V$ . We call  $\mathcal{M}$  the corresponding sheaf on  $J/V$ . This is a symmetric principal polarization. In particular,  $h^0(\mathcal{M}) = 1$  and there is a unique effective divisor  $Y$  on  $J/V$  associated with  $\mathcal{M}$ . We set  $X = f^*Y$ . This is an effective divisor linearly equivalent to  $lW_{-\theta}$  and invariant by  $V$ . Let  $\mathbf{u} = \sum_{1 \leq i \leq I} e_i[u_i]$  be a zero-cycle in  $J$ . Let  $y$  be a point on  $J$ . We assume that  $y$  does not belong to the support of the divisor  $\sum_{1 \leq i \leq I} e_i X_{u_i} - X_{s(\mathbf{u})} - (\deg(\mathbf{u}) - 1)X$ . Recall that  $\eta_X[\mathbf{u}, y]$  is the unique function on  $J$  having divisor

$$(\eta_X[\mathbf{u}, y]) = \sum_{1 \leq i \leq I} e_i X_{u_i} - X_{s(\mathbf{u})} - (\deg(\mathbf{u}) - 1)X$$

and such that

$$\eta_X[\mathbf{u}, y](y) = 1.$$

Set  $v_i = f(u_i) \in J/V$  for every  $1 \leq i \leq I$  and let  $\mathbf{v} = f(\mathbf{u}) = \sum_{1 \leq i \leq I} e_i[v_i]$  be the image of  $\mathbf{u}$  in the group of zero-cycles on  $J/V$ . There is a function with divisor  $\sum_{1 \leq i \leq I} e_i Y_{v_i} - Y_{s(\mathbf{v})} - (\deg(\mathbf{v}) - 1)Y$  on  $J/V$ . Composing this function with  $f$  we obtain a function on  $J$  having the same divisor as  $\eta_X[\mathbf{u}, y]$ . So  $\eta_X[\mathbf{u}, y]$  is invariant by  $V$  and can be identified with the unique function on  $J/V$  with divisor  $\sum_{1 \leq i \leq I} e_i Y_{v_i} - Y_{s(\mathbf{v})} - (\deg(\mathbf{v}) - 1)Y$ , and taking value 1 at  $f(y)$ . When dealing with the quotient  $J/V$  it will be useful to represent a point  $z$  on  $J/V$  by a point  $x$  on  $J$  such that  $f(x) = z$ . Such an  $x$  is in turn represented by a divisor  $D_x - gO$  on  $C$ . It is then natural to evaluate functions like  $\eta_X[\mathbf{u}, y]$  at such an  $x$ . For example, taking  $\mathbf{u} = m[u]$  for  $u$  an  $m$ -torsion point, the function  $\eta_X[\mathbf{u}, y]$  is essentially a Theta function of level  $m$  for the quotient  $J/V$ . Evaluating such functions at a few points, we find projective equations for  $J/V$ . This will show very useful in Section 6. Section 5.1 provides an expression of  $\eta_X[\mathbf{u}, y]$  as a product involving a function  $\Phi_V$  defined as an eigenvalue for the canonical lift of  $V$  in  $\mathcal{G}(\mathcal{L})$ . The complexity of evaluating  $\Phi_V$  is bounded in Section 5.2.

**5.1. Explicit descent.** We look for a function  $\Phi_V$  with divisor  $X - lW_{-\theta}$  on  $J$ . Let  $V^D = \text{Hom}(V, \mathbf{G}_m)$  be the dual of  $V$ . For every character  $\chi$  in  $V^D$  we denote  $H_\chi$  the 1-dimensional subspace of  $H^0(J, \mathcal{O}_J(lW_{-\theta}))$  where  $V$  acts through multiplication by  $\chi$ . Then

$$\mathbf{a}_V = \sum_{v \in V} \mathbf{a}_v$$

is a surjection from  $H^0(J, \mathcal{O}_J(lW_{-\theta}))$  onto  $H_1$ . We pick a random function in  $H^0(J, \mathcal{O}_J(lW_{-\theta}))$  as explained in Proposition 2, and apply  $\mathbf{a}_V$  to it. With probability  $\geq 1/2$  the resulting function is a non-zero function in  $H_1$ . We call this function  $\Phi_V$ . We will explain in Section 5.2 how to evaluate  $\Phi_V$  at a given point on  $J$ . We now explain how to express any  $\eta_X[\mathbf{u}]$  as a multiplicative combination of  $\Phi_V$  and its translates. Without loss of generality we can assume that  $s(\mathbf{u}) = 0$  and  $\deg(\mathbf{u}) = 0$ . We assume that  $y \notin \bigcup_i W_{-\theta+u_i} \cup \bigcup_i X_{u_i}$ . The composition  $\Phi_V \circ t_{-u_i}$  has divisor  $X_{u_i} - lW_{-\theta+u_i}$ . The composition  $\eta[\mathbf{u}, y + \vartheta] \circ t_\vartheta$  has divisor  $\sum_i e_i W_{-\theta+u_i}$ . So

$$\eta_X[\mathbf{u}, y](x) = (\eta[\mathbf{u}, y + \vartheta](x + \vartheta))^l \cdot \prod_{1 \leq i \leq I} (\Phi_V(x - u_i))^{e_i} \cdot \prod_{1 \leq i \leq I} (\Phi_V(y - u_i))^{-e_i}.$$

### 5.2. Evaluating functions on $J/V$ .

We now bound the cost of evaluating  $\Phi_V$  at a given point  $x \in J(\mathbf{K})$ . We assume that  $l$  is odd and prime to the characteristic  $p$  of  $\mathbf{K}$ . We are given two coprime integers  $a$  and  $b$  such that  $a + b = l$ , and two elements  $u$  and  $y$  in  $J(\mathbf{K})$  such that  $y \notin W_{-\theta} \cup W_{-\theta+au} \cup W_{-\theta-bu}$ . The function  $\Phi_V$  is the image by  $\mathbf{a}_V$  of some function  $\tau$  in  $H^0(J, \mathcal{O}_J(lW_{-\theta}))$ . We choose  $\tau$  to be the function

$$\tau = \tau[u, y + \vartheta] \circ t_\vartheta = \eta[b[au] + a[-bu], y + \vartheta] \circ t_\vartheta.$$

The  $\mathbf{K}$ -scheme  $V$  is given by a collection of field extensions  $(\mathbf{L}_i/\mathbf{K})_{1 \leq i \leq I}$  and a point  $w_i \in V(\mathbf{L}_i)$  for every  $i$  such that  $V$  is the disjoint union of the  $\mathbf{K}$ -Zariski closures of all  $w_i$ . In particular,  $\sum_i d_i = l^g$  where  $d_i$  is the degree of  $\mathbf{L}_i/\mathbf{K}$  and the  $\mathbf{L}_i$  are the minimum fields of definition for the  $w_i$ . Equivalently, we may be given a separable algebra  $\mathbf{L} = \mathbf{K}[V]$  of degree  $l^g$  over  $\mathbf{K}$  and a point

$$w \in V(\mathbf{L}) \subset J(\mathbf{L}).$$

We are given an element  $x$  in  $J(\mathbf{K})$  such that  $x \notin \cup_{w \in V} W_{-\theta+w}$ . The value

$$\mathbf{a}_w(\tau)(x) = \theta_w(x) \cdot \tau(x - w) = \theta_w(x) \cdot \eta[b[au] + a[-bu], y + \vartheta](x - w + \vartheta)$$

of  $\mathbf{a}_w(\tau)$  at  $x$  is an element of the affine algebra  $\mathbf{K}[V]$ . Its trace over  $\mathbf{K}$  is equal to  $\Phi_V(x)$ .

**Theorem 2** (Evaluating functions on quotients  $J/V$ ). *There exists a deterministic algorithm that takes as input*

- a finite field  $\mathbf{K}$  with characteristic  $p$  and cardinality  $q$ ,
- a curve  $C$  of genus  $g \geq 2$  over  $\mathbf{K}$ ,
- a zero-cycle  $\mathbf{u} = \sum_{1 \leq i \leq I} e_i[u_i]$  on the Jacobian  $J$  of  $C$  such that  $u_i \in J(\mathbf{K})$  for every  $1 \leq i \leq I$ ,  $\deg(\mathbf{u}) = 0$ , and  $s(\mathbf{u}) = 0$ ,
- a Theta characteristic  $\theta$  defined over  $\mathbf{K}$ ,
- an odd prime integer  $l \neq p$ ,
- a maximal isotropic  $\mathbf{K}$ -subgroup scheme  $V \subset J[l]$ ,
- two classes  $x$  and  $y$  in  $J(\mathbf{K})$  such that  $y \notin \cup_i W_{-\theta+u_i} \cup \cup_i X_{u_i}$ .

The algorithm returns either FAIL or  $\eta_X[\mathbf{u}, y](x)$  in time  $I \cdot (\log |e|) \cdot g^{\mathfrak{D}} \cdot (\log q)^{1+\epsilon(q)} \cdot l^{g(1+\epsilon(l^g))}$ , where  $|e| = \sum_{1 \leq i \leq I} |e_i|$  is the  $\ell^1$ -norm of  $e$ . For given  $\mathbf{K}$ ,  $C$ ,  $\mathbf{u}$ ,  $\theta$ ,  $V$  there exists a subset  $\mathbf{FAIL}(\mathbf{K}, C, \mathbf{u}, \theta, V)$  of  $J(\mathbf{K})$  with density  $\leq I \cdot (\log |e|) \cdot g^{\mathfrak{D}g} \cdot l^{g^2} \cdot (\log l)/q$  and such that the algorithm succeeds whenever none of  $x$  and  $y$  belongs to  $\mathbf{FAIL}(\mathbf{K}, C, \mathbf{u}, \theta, V)$ .

## 6. CURVES OF GENUS TWO

In this section we assume that the characteristic  $p$  of  $\mathbf{K}$  is odd. We bound the complexity of computing an isogeny  $J_C \rightarrow J_D$  between two Jacobians of dimension two. We give in Section 6.1 the expected form of such an isogeny. In Section 6.2 we characterize the isogeny as the solution of some system of differential equations. As a consequence of these differential equations we can compute such an isogeny in two steps: we first compute the image of a  $(\mathbf{K}[t]/t^3)$ -point on  $C$  by the isogeny, then lift to  $\mathbf{K}[[t]]$ . We explain in Section 6.3 how to compute images of points. The main result in this section is Theorem 3 below.



**6.1. Algebraic form of the isogeny.** Let  $C$  be a projective, smooth, absolutely integral curve of genus 2 over  $\mathbf{K}$ . We assume that  $C$  is given by the affine singular model

$$(10) \quad v^2 = h_C(u)$$

where  $h_C$  is a polynomial of degree 5. Let  $O_C$  be the unique place at infinity. Let  $J_C$  be the Jacobian of  $C$  and let  $j_C : C \rightarrow J_C$  be the Jacobi map with origin  $O_C$ . The image of a point  $P$  on  $C$  by  $j_C$  is the class of  $P - O_C$ . Let  $D$  be another projective, smooth, absolutely irreducible curve of genus 2 over  $\mathbf{K}$ . We assume that  $D$  is given by the affine singular model  $y^2 = h_D(x)$  where  $h_D$  is a polynomial of degree 5 or 6. Let  $K_D$  be a canonical divisor on  $D$ . Call  $D^{(2)}$  the symmetric square of  $D$  and let  $j_D^{(2)} : D^{(2)} \rightarrow J_D$  be the map sending the pair  $\{Q_1, Q_2\}$  onto the class  $z = j_D^{(2)}(\{Q_1, Q_2\})$  of  $Q_1 + Q_2 - K_D$ . This is a birational morphism. We define the Mumford coordinates

$$\begin{aligned} \mathbf{s}(z) &= x(Q_1) + x(Q_2), \\ \mathbf{p}(z) &= x(Q_1) \cdot x(Q_2), \\ \mathbf{q}(z) &= y(Q_1) \cdot y(Q_2), \\ \mathbf{r}(z) &= (y(Q_2) - y(Q_1)) / (x(Q_2) - x(Q_1)). \end{aligned}$$

The function field of  $J_D$  is  $\mathbf{K}(\mathbf{s}, \mathbf{p}, \mathbf{q}, \mathbf{r})$ . The function field of the Kummer variety of  $D$  is  $\mathbf{K}(\mathbf{s}, \mathbf{p}, \mathbf{q})$ . We assume that there exists an isogeny  $f : J_C \rightarrow J_D$  with kernel  $V$ , a maximal isotropic group in  $J_C[l]$ , where  $l$  is an odd prime different from the characteristic  $p$  of  $\mathbf{K}$ . We define  $F : C \rightarrow J_D$  to be the composite map  $f \circ j_C$ . There exists a unique morphism  $G : C \rightarrow D^{(2)}$  such that the following diagram commutes.

$$\begin{array}{ccc} & & D^{(2)} \\ & \nearrow G & \downarrow j_D^{(2)} \\ C & & J_D \\ & \searrow F & \end{array}$$

For every point  $P = (u, v)$  on  $C$  we have  $F((u, -v)) = -F(P)$ . We deduce the following algebraic description of the map  $F$

$$(11) \quad \begin{aligned} \mathbf{s}(F(P)) &= \mathbf{S}(u), \\ \mathbf{p}(F(P)) &= \mathbf{P}(u), \\ \mathbf{q}(F(P)) &= \mathbf{Q}(u), \\ \mathbf{r}(F(P)) &= v\mathbf{R}(u), \end{aligned}$$

where  $\mathbf{S}, \mathbf{P}, \mathbf{Q}, \mathbf{R}$  are rational fractions in one variable. Let  $O_D$  be a point on  $D$ . Let  $Z$  be the algebraic subset of  $D^{(2)}$  consisting of pairs  $\{O_D, Q\}$  for some  $Q$  in  $D$ . Let  $T \subset J_D$  be the image of  $Z$  by  $j_D^{(2)}$ . This is a divisor with self intersection

$$T.T = 2.$$

The image  $F(C)$  of  $C$  by  $F$  is algebraically equivalent to  $lT$ . The divisors of poles of the functions  $s$ ,  $p$ ,  $q$ , and  $r$ , are algebraically equivalent to  $2T$ ,  $2T$ ,  $6T$ , and  $4T$ , respectively. Seen as functions on  $C$ , the functions  $S(u)$ ,  $P(u)$ ,  $Q(u)$ , and  $vR(u)$ , thus have degrees bounded by  $4l$ ,  $4l$ ,  $12l$ , and  $8l$ , respectively. So the rational fractions  $S$ ,  $P$ ,  $Q$ , and  $R$ , have degrees bounded by  $2l$ ,  $2l$ ,  $6l$ , and  $4l + 3$ , respectively. The four rational fractions  $S$ ,  $P$ ,  $Q$ ,  $R$  provide a compact description of the isogeny  $f$  from which we can deduce any desirable information about it.

**6.2. Associated differential system.** The morphism  $F : C \rightarrow J_D$  induces a map

$$F^* : H^0(J_D, \Omega_{J_D/\mathbf{K}}^1) \rightarrow H^0(C, \Omega_{C/\mathbf{K}}^1).$$

So the vector  $(S, P, Q, R)$  satisfies a first order differential system. This system can be given a convenient form using local coordinates. A basis for  $H^0(C, \Omega_{C/\mathbf{K}}^1)$  is made of  $du/v$  and  $udu/v$ . We identify  $H^0(J_D, \Omega_{J_D/\mathbf{K}}^1)$  with the invariant subspace of  $H^0(D \times D, \Omega_{D \times D/\mathbf{K}}^1)$  by the permutation of the two factors. We deduce that a basis for this space is made of  $dx_1/y_1 + dx_2/y_2$  and  $x_1 dx_1/y_1 + x_2 dx_2/y_2$ . Let  $M = (m_{i,j})_{1 \leq i,j \leq 2}$  be the matrix of  $F^*$  with respect to these two bases. So

$$(12) \quad \begin{aligned} F^*(dx_1/y_1 + dx_2/y_2) &= (m_{1,1} + m_{2,1}.u).du/v, \\ F^*(x_1 dx_1/y_1 + x_2 dx_2/y_2) &= (m_{1,2} + m_{2,2}.u).du/v. \end{aligned}$$

Let  $P = (u_P, v_P)$  be a point on  $C$ . We assume that  $v_P \neq 0$ . Let  $Q_1$  and  $Q_2$  be two points on  $D$  such that  $F(P)$  is the class of  $Q_1 + Q_2 - K_D$ . We assume that  $F(P) \neq 0$ , so the divisor  $Q_1 + Q_2$  is non-special. We also assume that  $Q_1 \neq Q_2$  and either of the points are defined over  $\mathbf{K}$ . Let  $t$  be a formal parameter. Set  $\mathbf{L} = \mathbf{K}((t))$ . We call

$$P(t) = (u(t), v(t))$$

the point on  $C(\mathbf{L})$  corresponding to the value  $t$  of the local parameter  $u - u_P$  at  $P$ . The image of  $P(t)$  by  $F$  is the class of  $Q_1(t) + Q_2(t) - K_D$  where  $Q_1(t)$  and  $Q_2(t)$  are two  $\mathbf{L}$ -points on  $D$ .

$$(13) \quad \begin{array}{ccc} \text{Spec } \mathbf{K}[[t]] & \xrightarrow{t \mapsto (Q_1(t), Q_2(t))} & D \times D \\ \downarrow t \mapsto P(t) & & \downarrow \\ C & \xrightarrow{F} & J_D. \end{array}$$

From Equations (12) and the commutativity of diagram (13) we deduce that the coordinates  $(x_1(t), y_1(t))$  and  $(x_2(t), y_2(t))$  of  $Q_1(t)$  and  $Q_2(t)$  satisfy the following non-singular first order system of differential equations.

$$(14) \quad \left\{ \begin{aligned} \frac{\dot{x}_1(t)}{y_1(t)} + \frac{\dot{x}_2(t)}{y_2(t)} &= \frac{(m_{1,1} + m_{2,1}.u(t)).\dot{u}(t)}{v(t)}, \\ \frac{x_1(t).\dot{x}_1(t)}{y_1(t)} + \frac{x_2(t).\dot{x}_2(t)}{y_2(t)} &= \frac{(m_{1,2} + m_{2,2}.u(t)).\dot{u}(t)}{v(t)}, \\ y_1(t)^2 &= h_D(x_1(t)), \\ y_2(t)^2 &= h_D(x_2(t)). \end{aligned} \right.$$

So we can recover the complete description of the isogeny, namely the rational fractions  $S$ ,  $P$ ,  $Q$ ,  $R$ , from the knowledge of the image by  $F$  of a *single* formal point on  $C$ . More concretely,

we compute the image  $\{Q_1(t), Q_2(t)\}$  of  $P(t)$  by  $G$  with low accuracy, then deduce from Equation (14) the values of the four scalars  $m_{1,1}, m_{1,2}, m_{2,1}, m_{2,2}$ . Then use Equation (14) again to increase the accuracy of the formal expansions up to  $O(t^{\mathfrak{D}l})$  and recover the rational fractions from their expansions using continued fractions. Coefficients of  $x_1(t)$  and  $x_2(t)$  can be computed one by one using Equation (14). Reaching accuracy  $\mathfrak{D}l$  then requires  $\mathfrak{D}l^2$  operations in  $\mathbf{K}$ . We can also use more advanced methods [5, 4] with quasi-linear complexity in the expected accuracy of the result. Both methods may produce zero denominators if the characteristic is small. In that case we use a trick introduced by Joux and Lercier [17] in the context of elliptic curves. We lift to a  $p$ -adic field having  $\mathbf{K}$  as residue field. The denominators introduced by (14) do not exceed  $p^{\mathfrak{D} \log(l)}$ . The required  $p$ -adic accuracy, and the impact on the complexity are thus negligible.

**6.3. Computing isogenies.** We are given a curve  $C$  of genus two, a Weierstrass point  $O_C$  and a maximal isotropic subspace  $V$  in  $J_C[l]$ . We set

$$A = J_C/V.$$

Since  $2O_C$  is a canonical divisor we set  $\theta = O_C$ . Using this Theta characteristic we define a principal polarization  $Y$  on  $A$  as in Section 5. We use the methods given in Sections 3 and 5 to find nine functions  $\eta_0 = 1, \eta_1, \dots, \eta_8$ , such that  $(\eta_0, \eta_1, \eta_2, \eta_3)$  is a basis of  $H^0(A, \mathcal{O}_A(2Y))$  and  $(\eta_0, \dots, \eta_8)$  is a basis of  $H^0(A, \mathcal{O}_A(3Y))$ . We thus define two maps  $e_2 : A \rightarrow \mathbf{P}^3$  and  $e_3 : A \rightarrow \mathbf{P}^8$ . Denoting  $\pi : \mathbf{P}^8 \dashrightarrow \mathbf{P}^3$  the projection

$$\pi(Z_0 : Z_1 : \dots : Z_8) = (Z_0 : Z_1 : Z_2 : Z_3)$$

we have  $\pi \circ e_3 = e_2$ . Evaluating the  $(\eta_i)_{0 \leq i \leq 8}$  at enough points we find equations for  $e_3(A)$  and  $e_2(A)$ . The intersection of  $e_3(A)$  with the hyperplane  $H_0$  with equation  $Z_0 = 0$  in  $\mathbf{P}^8$  is  $e_3(Y)$  counted with multiplicity 3. We now assume that  $Y$  is a smooth and absolutely integral curve of genus two. This is the generic case, and it is true in particular whenever the Jacobian  $J_C$  of  $C$  is absolutely simple. The intersection of  $e_2(A)$  with the hyperplane with equation  $Z_0 = 0$  in  $\mathbf{P}^3$  is  $e_2(Y)$  counted with multiplicity 2. The map  $Y \rightarrow e_2(Y)$  is the hyperelliptic quotient. It has degree two. Its image  $e_2(Y)$  is a plane curve of degree two. We deduce explicit equations for a hyperelliptic curve  $D$  and an isomorphism  $D \rightarrow Y$ .

We now define a rational map  $\varphi$  from  $J_C$  into the symmetric square of  $D \simeq Y$  by setting, for  $z$  a generic point on  $J_C$ ,

$$(15) \quad \varphi(z) = Y_{f(z)} \cap Y,$$

where  $Y_{f(z)}$  is the translate of  $Y$  by  $f(z)$ . Recall that  $O_C$  is a Weierstrass point on  $C$ . We define a map  $\psi$  from  $C$  into the symmetric square of  $D \simeq Y$  by setting, for  $P \in C$  a generic point,  $\psi(P) = \varphi(P - O_C)$ . We check that  $\psi(O_C)$  is a canonical divisor  $K_Y$  on  $Y$ . The difference  $\psi(P) - \psi(O_C)$  is a degree 0 divisor on  $Y$  and belongs to the class  $f(P - O_C)$ . So  $\psi : C \rightarrow Y^{(2)}$  is the map  $G$  introduced in Section 6.1.

We explain how to evaluate the map  $\varphi$  at a given  $z$  in  $J_C$ . The main point is to compute the intersection in Equation (15). This is a matter of linear algebra. We pick two auxiliary classes  $z_1$  and  $z_2$  in  $J_C$ . We set  $z'_1 = -z - z_1$  and  $z'_2 = -z - z_2$ . We assume that  $\varphi(z_1), \varphi(z_2), \varphi(z'_1), \varphi(z'_2)$  are pairwise disjoint. Seen as a function on  $A = J_C/V$ , the function  $\eta_X[[z_1] + [z'_1] + [z]]$  belongs

to  $H^0(A, \mathcal{O}_A(3Y))$ . Evaluating it at a few points we can express it as a linear combination of the elements  $(\eta_i)_{0 \leq i \leq 8}$  of our basis:

$$\eta_X[[z_1] + [z'_1] + [z]] = \sum_{0 \leq i \leq 8} c_i \cdot \eta_i.$$

The hyperplane section  $H_1$  with equation  $\sum_i c_i Z_i = 0$  intersects  $e_3(A)$  at  $Y_{f(z_1)} \cup Y_{f(z'_1)} \cup Y_{f(z)}$ . We similarly find an hyperplane section  $H_2$  with equation  $\sum_i d_i Z_i = 0$  intersecting  $e_3(A)$  at  $Y_{f(z_2)} \cup Y_{f(z'_2)} \cup Y_{f(z)}$ . So

$$\varphi(z) = Y_{f(z)} \cap Y = H_1 \cap H_2 \cap H_0 \cap e_3(A),$$

is computed by linear substitutions. Altogether we have proven the theorem below.

**Theorem 3** (Computing isogenies for genus two curves). *There exists a probabilistic (Las Vegas) algorithm that takes as input*

- a finite field  $\mathbf{K}$  of odd characteristic  $p$ , and cardinality  $q$ ,
- an odd prime  $l$  different from  $p$ ,
- a projective, smooth, absolutely irreducible curve of genus two,  $C$ , given by a plane affine singular model as in Equation (10),
- a maximal isotropic subgroup  $V$  in  $J_C[l]$  as in Section 5.2, such that the curve  $Y$  introduced in Section 5 is smooth and absolutely integral.

*The algorithm returns a genus two curve  $D$  and a map  $F : C \rightarrow J_D$  as in Equation (11). The running time is  $l^{2+\epsilon(l)} \cdot (\log q)^{1+\epsilon(q)}$ .*

In case  $Y$  is not smooth and absolutely integral, it is a stable curve of genus two. The calculation above will work just as well and produce one map from  $C$  onto either of the components of  $Y$ . We do not formalize this degenerate case.

## 7. AN EXAMPLE

Let  $\mathbf{K}$  be the field with 1009 elements. Let

$$h_C(u) = u(u-1)(u-2)(u-3)(u-85) \in \mathbf{K}[u]$$

and let  $C$  be the projective, smooth, absolutely irreducible curve of genus two given by the singular plane model with equation  $v^2 = h_C(u)$ . Let  $O_C$  be the place at infinity. Let  $o_C$  be the corresponding class in  $\text{Pic}^1(C)$ . Let  $T_1$  be the effective divisor of degree 2 defined by the ideal

$$(u^2 + 247u + 67, v - 599 - 261u) \subset \mathbf{K}[u, v]/(v^2 - h_C(u)).$$

Let  $T_2$  be the effective divisor of degree 2 defined by the ideal

$$(u^2 + 903u + 350, v - 692 - 98u) \subset \mathbf{K}[u, v]/(v^2 - h_C(u)).$$

The classes of  $T_1 - 2O_C$  and  $T_2 - 2O_C$  generate a totally isotropic subspace  $V$  of dimension 2 inside  $J_C[3]$ . Let  $A = J_C/V$ . Let  $W_{-o_C} \subset J_C$  be the set of classes of divisors  $P - O_C$  for  $P$  a point on  $C$ . Since  $O_C$  is a Weierstrass point, we have  $[-1]^* W_{-o_C} = W_{-o_C}$ . Let  $X \subset J_C$  and  $Y \subset A$  be the two divisors introduced at the beginning of Section 5. Let  $B \subset C$  be the effective divisor of degree 2 defined by the ideal  $(u^2 + 862u + 49, v - 294 - 602u)$ . Let  $b \in J_C(\mathbf{K})$  be the class of

$B - 2O_C$ . For  $i$  in  $\{0, 1, 2, 3, 85\}$  let  $P_i$  be the point on  $C$  with coordinates  $u = i$  and  $v = 0$ . The class of  $P_i$  in  $\text{Pic}^1(C)$  is denoted  $p_i$ . We set  $p_\infty = o_C$  and  $p_+ = p_0 + p_1 - o_C \in \text{Pic}^1(C)$ .

For  $i$  in  $\{\infty, 0, 1, +, 2, 3, 85\}$  let  $\eta_i$  be the unique function on  $J_C$  with divisor  $2(X_{p_i - o_C} - X)$  and taking value 1 at  $b$ . These functions are invariant by  $V$  and may be seen as level two Theta functions on  $A$ . Evaluating these functions at a few points we check that  $(\eta_\infty, \eta_0, \eta_1, \eta_+)$  form a basis of  $H^0(A, \mathcal{O}_A(2Y))$  and

$$\begin{aligned}\eta_2 &= 437\eta_\infty + 241\eta_0 + 332\eta_1, \\ \eta_3 &= 294\eta_\infty + 246\eta_0 + 470\eta_1, \\ \eta_{85} &= 639\eta_\infty + 827\eta_0 + 553\eta_1.\end{aligned}$$

Call  $Z_\infty, Z_0, Z_1, Z_+$  the projective coordinates associated with  $(\eta_\infty, \eta_0, \eta_1, \eta_+)$ . The Kummer surface of  $A$  is defined by the vanishing of the following homogeneous form of degree four

$$\begin{aligned}&597Z_\infty^2Z_0^2 + 14Z_\infty^2Z_0Z_1 + 781Z_\infty^2Z_0Z_+ + 819Z_\infty^2Z_1Z_+ + 835Z_\infty^2Z_1^2 + 615Z_\infty^2Z_+^2 \\ &+ 401Z_\infty Z_0^2Z_1 + 833Z_\infty Z_0^2Z_+ + 553Z_\infty Z_0Z_1Z_+ + 843Z_\infty Z_0Z_1^2 + 206Z_\infty Z_0Z_+^2 + 418Z_\infty Z_1^2Z_+ \\ &+ 321Z_\infty Z_1Z_+^2 + 796Z_0^2Z_1Z_+ + Z_0^2Z_1^2 + 1000Z_0^2Z_+^2 + 856Z_0Z_1^2Z_+ + 655Z_0Z_1Z_+^2 + 555Z_1^2Z_+^2.\end{aligned}$$

This equation is found by evaluating all four functions at forty points. We set  $Z_\infty = 0$  in this form and find the square of the following quadratic form

$$(16) \quad 611Z_0Z_+ + 581Z_1Z_+ - Z_0Z_1$$

which is an equation for  $e_2(Y)$  in the projective plane  $Z_\infty = 0$ . Recall  $e_2 : A \rightarrow \mathbf{P}^3$  is the map introduced in Section 6.3. Set

$$\begin{aligned}Z_2 &= 437Z_\infty + 241Z_0 + 332Z_1 \\ Z_3 &= 294Z_\infty + 246Z_0 + 470Z_1 \\ Z_{85} &= 639Z_\infty + 827Z_0 + 553Z_1.\end{aligned}$$

We find an affine parameterization of the conic  $e_2(Y)$  in Equation (16) by setting

$$Z_+ = 1 \text{ and } Z_1 = xZ_0.$$

For  $i$  in  $\{0, 1, +, 2, 3, 85\}$  call  $D_i$  the line with equations  $\{Z_\infty = 0, Z_i = 0\}$ . There are six intersection points between  $e_2(Y)$  and one of the  $D_i$ . These are the six branched points of the hyperelliptic cover  $Y \rightarrow e_2(Y)$ . They correspond to the values

$$\{0, \infty, 513, 51, 243, 987\}$$

of the  $x$  parameter. We set

$$h_D(x) = x(x - 513)(x - 51)(x - 243)(x - 987) \in \mathbf{K}[x]$$

and let  $D$  be the genus two curve given by the singular plane model with equation  $y^2 = h_D(x)$ . Let  $O_D$  be the unique place at infinity on  $D$ . Let  $P = (u, v)$  be a point on  $C$ . Using notation introduced in Section 6.1 we call  $F(P)$  the image of  $P - O_C$  in  $J_D$  and  $G(P)$  an effective divisor such that  $F(P) = G(P) - 2O_D$ . This divisor is defined by the ideal

$$(x^2 - \mathbf{S}(u)x + \mathbf{P}(u), y - v(\mathbf{T}(u) + x\mathbf{R}(u))) \subset \mathbf{K}(u, v)[x, y]/(y^2 - h_D(x))$$

where

$$\begin{aligned} \mathbf{S}(u) &= 354 \frac{u^5 + 647u^4 + 931u^3 + 597u^2 + 73u + 361}{u^5 + 832u^4 + 811u^3 + 215u^2 + 420u}, \\ \mathbf{P}(u) &= 50 \frac{u^5 + 262u^4 + 812u^3 + 770u^2 + 868u + 314}{u^5 + 832u^4 + 811u^3 + 215u^2 + 420u}, \\ \mathbf{R}(u) &= 304 \frac{u^6 + 437u^5 + 623u^4 + 64u^3 + 194u^2 + 3u + 511}{u^8 + 239u^7 + 983u^6 + 800u^5 + 214u^4 + 489u^3 + 191u^2}, \\ \mathbf{T}(u) &= 678 \frac{u^6 + 697u^5 + 263u^4 + 895u^3 + 859u^2 + 204u + 130}{u^8 + 239u^7 + 983u^6 + 800u^5 + 214u^4 + 489u^3 + 191u^2}. \end{aligned}$$

We note that the fraction  $\mathbf{Q}(u)$  introduced in Section 6.1 is

$$\mathbf{Q} = h_C \cdot (\mathbf{T}^2 + \mathbf{R}^2 \cdot \mathbf{P} + \mathbf{S} \cdot \mathbf{R} \cdot \mathbf{T}).$$

We now explain how these rational fractions were computed. We consider the formal point

$$P(t) = (u(t), v(t)) = (832 + t, 361 + 10t + 14t^2 + O(t^3))$$

on  $C$ . We compute  $G(P(t)) = \{Q_1(t), Q_2(t)\}$  and find

$$\begin{aligned} Q_1(t) &= (x_1(t), y_1(t)) = (973 + 889t + 57t^2 + O(t^3), 45 + 209t + 39t^2 + O(t^3)), \\ Q_2(t) &= (x_2(t), y_2(t)) = (946 + 897t + 252t^2 + O(t^3), 911 + 973t + 734t^2 + O(t^3)). \end{aligned}$$

Using Equation (14) we deduce the values

$$m_{1,1} = 186, m_{1,2} = 864, m_{2,1} = 853, m_{2,2} = 640.$$

Using Equation (14) again we increase the accuracy in the expansions for  $x_1(t)$ ,  $x_2(t)$ ,  $y_1(t)$ , and  $y_2(t)$  then deduce the rational fractions  $\mathbf{S}$ ,  $\mathbf{P}$ ,  $\mathbf{R}$ , and  $\mathbf{T}$ .

## REFERENCES

- [1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I*, volume 267 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, New York, 1985.
- [2] H F Baker. *Abel's theorem and the allied theory, including the theory of the theta functions*. Cambridge Univ. Press, Cambridge, 1897.
- [3] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 2004.
- [4] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp.*, 77(263):1755–1778, 2008.
- [5] R. P. Brent and H. T. Kung. Fast algorithms for manipulating formal power series. *J. Assoc. Comput. Mach.*, 25(4):581–595, 1978.
- [6] Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1997. With the collaboration of Thomas Lickteig.
- [7] Romain Cosset and Damien Robert. Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves. to appear in *Mathematics of Computations*, October 2013.
- [8] Jean-Marc Couveignes. Computing  $V_f$  modulo  $p$ . In *Computational aspects of modular forms and Galois representations*, volume 176 of *Ann. of Math. Stud.*, pages 337–370. Princeton Univ. Press, Princeton, NJ, 2011.

- [9] Jean-Marc Couveignes and Bas Edixhoven. First description of the algorithms. In *Computational aspects of modular forms and Galois representations*, volume 176 of *Ann. of Math. Stud.*, pages 69–78. Princeton Univ. Press, Princeton, NJ, 2011.
- [10] Claus Diem. *On arithmetic and the discrete logarithm problem in class groups of curves*. Habilitation thesis. Leipzig, 2008.
- [11] I. Dolgachev and D. Lehavi. On isogenous principally polarized abelian surfaces. In *Curves and abelian varieties*, volume 465 of *Contemp. Math.*, pages 51–69. Amer. Math. Soc., Providence, RI, 2008.
- [12] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.
- [13] John D. Fay. *Theta Functions on Riemann Surfaces*. Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, Vol. 352.
- [14] François Le Gall. Powers of tensors and fast matrix multiplication. *CoRR*, abs/1401.7714, 2014.
- [15] Sudhir R. Ghorpade and Gilles Lachaud. Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. *Mosc. Math. J.*, 2(3):589–631, 2002. Dedicated to Yuri I. Manin on the occasion of his 65th birthday.
- [16] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.
- [17] Antoine Joux and Reynald Lercier. Counting points on elliptic curves in medium characteristic. Cryptology ePrint Archive, Report 2006/176, 2006.
- [18] Kamal Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Math. Comp.*, 76(260):2213–2239, 2007.
- [19] Gilles Lachaud and Mireille Martin-Deschamps. Nombre de points des jacobiniennes sur un corps fini. *Acta Arith.*, 56(4):329–340, 1990.
- [20] Serge Lang. *Abelian varieties*. Springer-Verlag, New York-Berlin, 1983. Reprint of the 1959 original.
- [21] R. Lercier and F. Morain. Algorithms for computing isogenies between elliptic curves. In D.A. Buell and J.T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 77–96, Providence, 1998. American Mathematical Society & International Press. Held in 1995 at the University of Illinois at Chicago.
- [22] David Lubicz and Damien Robert. Computing isogenies between abelian varieties. *Compos. Math.*, 148(5):1483–1515, 2012.
- [23] David Lubicz and Damien Robert. Computing separable isogenies in quasi-optimal time. February 2014.
- [24] Nicolas Mascot. Computing modular Galois representations. *Rend. Circ. Mat. Palermo (2)*, 62(3):451–476, 2013.
- [25] Victor S. Miller. The Weil pairing, and its efficient calculation. *J. Cryptology*, 17(4):235–261, 2004.
- [26] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.
- [27] David Mumford. *Tata lectures on theta. III*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. With collaboration of Madhav Nori and Peter Norman, Reprint of the 1991 original.
- [28] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.
- [29] René Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).
- [30] N. Shepherd-Barron. Thomae’s formulae for non-hyperelliptic curves and spinorial square roots of theta-constants on the moduli space of curves. *ArXiv e-prints*, February 2008.
- [31] Benjamin Smith. Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method. In *Arithmetic, geometry, cryptography and coding theory*, volume 574 of *Contemp. Math.*, pages 159–170. Amer. Math. Soc., Providence, RI, 2012.

- [32] The PARI Group, Bordeaux. *PARI/GP version 2.7.2*, 2014. available from <http://pari.math.u-bordeaux.fr/>.
- [33] Jacques V  lu. Isog  nies entre courbes elliptiques. *C. R. Acad. Sci. Paris S  r. A-B*, 273:A238–A241, 1971.
- [34] Jacques V  lu. Courbes elliptiques munies d’un sous-groupe  $\mathbf{Z}/n\mathbf{Z} \times \mu_n$ . *Bull. Soc. Math. France M  m.*, (57):5–152, 1978.
- [35] Andr   Weil. *Sur les courbes alg  briques et les vari  t  s qui s’en d  duisent*. Actualit  s Sci. Ind., no. 1041, Publ. Inst. Math. Univ. Strasbourg 7 (1945). Hermann et Cie., Paris, 1948.
- [36] Andr   Weil. *Vari  t  s ab  liennes et courbes alg  briques*. Actualit  s Sci. Ind., no. 1064, Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, BORDEAUX INP, CNRS, IMB, UMR 5251, F-33400 TALENCE, FRANCE.

JEAN-MARC COUVEIGNES, INRIA, LFANT, LIRIMA, F-33400 TALENCE, FRANCE.  
*E-mail address:* Jean-Marc.Couveignes@u-bordeaux.fr

TONY EZOME, UNIVERSIT   DES SCIENCES ET TECHNIQUES DE MASUKU, FACULT   DES SCIENCES, D  PARTEMENT DE MATH  MATIQUES ET INFORMATIQUE, BP 943 FRANCEVILLE, GABON.

TONY EZOME, INRIA, LIRIMA  
*E-mail address:* latonyo2000@yahoo.fr